A WWW SERVICE TO EMBED AND PROVE DIGITAL COPYRIGHT WATERMARKS

Jian Zhao

Fraunhofer Institute for Computer Graphics
Wilhelminenstr. 7, 64283 Darmstadt
GERMANY
Email: zhao@igd.fhg.de

ABSTRACT

This paper describes a digital watermarking service which allows the publisher and information provider to mark and identify their copyrighted materials through the World Wide Web (WWW). First a general copyright watermarking scheme is proposed to aim at identifying the ownership and distribution path of multimedia works. Then a class of digital watermarking methods for images, videos and structured texts is outlined. Finally the implementation of this watermarking scheme in the WWW is described.

Keywords: Copyright Protection, Digital Watermarking, World Wide Web, Multimedia.

1 INTRODUCTION

The intrinsic characteristics of digital media (such as ease of replication, ease of transmission and multiple use, plasticity, identical copying, compactness and nonlinearity) have caused the problems associated with the enforcement of intellectual property rights [1, 2, 3]. One of the major solutions to the problems is based on *usage control scheme*, i.e. each usage such as printing, viewing or playing of the copyright protected material is controlled by authorized "rendering" hardware, firmware or programs. This scheme has been recommended by the working group on intellectual property rights in the USA's National Information Infrastructure [4]. A similar scheme, called CITED model, has even been experimentally implemented in CITED [5] and COPICAT [6] projects funded by the European Commission.

Although such restrictive use scheme may become the predominant transaction in some applications such as video-on-demand, it seems unlikely that it will be the single universal

solution. For example, P. Samuelson has criticized the scheme and concluded in some fields, e.g. in digital libraries, that the usage-based scheme is inappropriate [7]. The reason is two-fold: first tolerating some leakage may be in the long run of the interest of publishers. Second it may deter learning and deep scholarship for educational and research work. Furthermore, this scheme may also cause legal and implementation problems. To implement such a use-control scheme, all user's rendering devices (e.g. for printing, displaying) and their production must be licensed and authorized. This prerequisite is difficult to meet without a harmonic standard, a moderate user acceptability, and corresponding legislation measures. Therefore, it is unlikely that as a universal solution this use-control scheme will be widely put into practice in near future.

Rather than attempt to restrict and control copying or use of copyrighted materials, another solution could be to allow unlimited copying or use, and afterwards to provide evidence of any misbehavior. This solution is based on digital copyright watermarking technique [8, 9, 10, 11, 12], which secretly embeds robust marks into a material to designate its copyrights-related information such as the origin, owner, content, use, or destinations. We believe that this technique on the one hand can provide evidence for copyright infringements after the event, on the other hand, it may serve as a kind of deterrent to illicit copying and dissemination of copyrighted materials, therefore, to decrease their occurrences in advance. In addition, the watermarking technique is not contrary to the usage-control scheme: it is just complementary to the usage-control scheme by providing another defence against misbehavior on the copyrighted materials that may escaped from the controlled domain of the usage-control scheme.

To makes the unauthorized copying and distribution evidential and provable, the copyright watermarking technique must meet the following requirements. First the embedded watermarks must be perpetual invisible, undetectable, unremovable and unalterable. Second it must be resistant against any processing and attack that do not effect the quality of the material. These requirements have been discussed in [3, 12].

To use digital watermarking, the copyright holders, especially small publishers and individual artists, expect a trusted body providing services

- to watermark and register copyrighted works,
- to provide copyrights and related information (such author, price) of a registered work,
- to verify the rights in the works, or
- to provide evidences of illegal copying and use.

The increasingly availability of computers, high-speed networks, and electronic commerce technology make the electronic service possible. The aim of the watermarking server pres-

ented in the paper is to automate these services through network means. This server first allows work owners in the network to watermark and verify their works without having watermarking softwares, second allows consumers to obtain copyright information of any registered (watermarked) work. Besides the watermarking service, such a server may provide more functionalities for facilitating electronic copyright transaction and clearance.

This paper presents a design of such a watermarking server and an implementation in the World Wide Web. We will first describe a general and flexible copyright watermarking scheme aiming to identify the ownership and distribution path of the copyrighted material. Then we briefly describe a variety of watermarking methods which are used to provide the watermarking services and have been developed in the SysCoP (System for Copyright Protection) [12]. Finally, an implementation of the watermarking server in the World Wide Web is described.

2 A COPYRIGHT WATERMARKING SCHEME

In this section, we propose a three-phase copyright watermarking scheme. This scheme is based on a belief in private control of copyrights only by respective owners, and in flexibility and freedom of copyright protection and management. All keys for reading watermarks and the original copy of the work are controlled by its copyright holder. We believe that any "key escrow" or "escrow of the original" is not the interest of complex and dynamic digital marketplace. The watermarking server in this scheme is a trusted assistant to provide flexible watermarking services. The owner can ask the server to watermark his works, or can watermark by himself locally and register the watermarking on the server, or even does not contact the server.

This scheme addresses two important identifications associated with copyrights in the work: the owner and the distribution. In addition, it proposes to embed a public watermark into the work to indicate its copyright notice.

Public watermark

Similar to a traditional copyright notice or indication, a public watermark is readable publicly, and may be displayed or performed by the rendering device (image viewer, audio or video player). More information such as price or contact address may further facilitate end users to receive or purchase a particular permission from the copyright holder. Unlike the watermarks for identifying the owner or recipient, the public watermark is not secure, but can help the end user who wants to know if a multimedia material is copyrighted and more (e.g. the rights of use, contact address), thus to decrease copyright infringements resulting from ignorance or carelessness of the users.

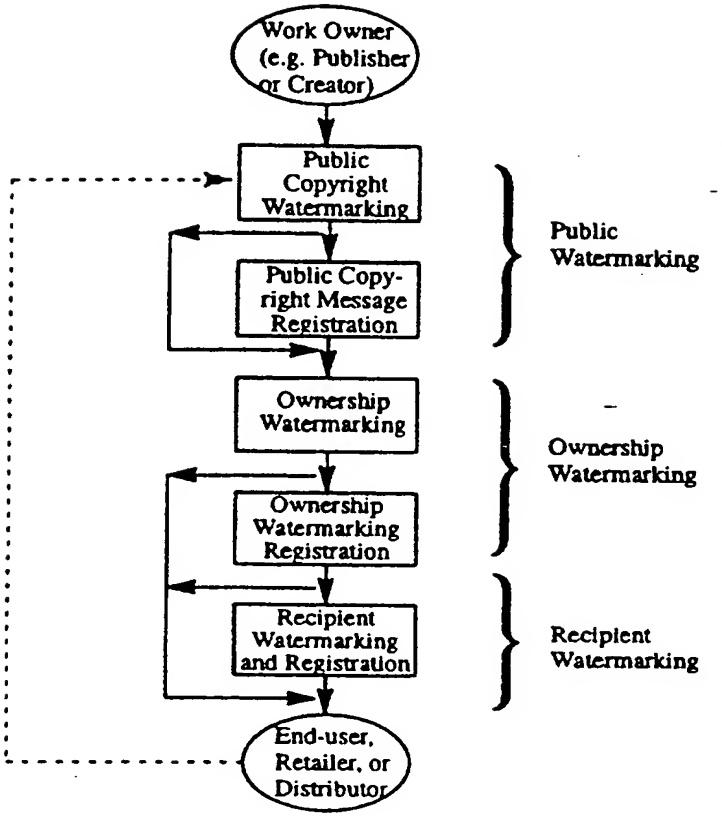

Figure 1. A digital copyright watermarking scheme

Ownership watermarking

This phase is concerned with the ownership watermarking and registration of the copyrighted material. The copyright holders have three optional ways to watermark their works:

- to send the work to the server for watermarking and registration,
- to watermark the work locally and then register this watermarking to the server, or
- to watermark and register the work locally.

More involvement of the watermarking server, more service can be provided to work holders and customers. In the first case, the server can not only provide copyright information, but can also solve some copyright disputes. In the last case the server only plays a role to read watermark from a work regardless of its authenticity. Section 4 will discuss watermark verification in details.

Recipient watermarking

This phase is optional – it embeds a unique identifier of a recipient into the material that will be delivered to the purchaser. It is likely to carry out this watermarking locally in information provider's site because of the large number of customers. A local codebook can be maintained to keep the mapping between customers' information and their unique identifiers. This recipient watermarking enables us to identify who made illicit copying and distribution.

When the recipients (i.e. purchasers) of the watermarked work are non-end-users (e.g. retailers or distributors), they may apply the second phase "recipient watermarking" again for their redistributions. Furthermore, when they buy the reproduction or derivation rights in the work from the original owner to produce or derive new materials, they have to perform the first phase "ownership watermarking" to protect their rights they bought in the new materials. Such a "multiple" ownerships and recipients chain implies another important requirement of digital watermarking: hierarchical watermarking, i.e. a multimedia data can be marked more than one times such that all watermarks are extractable if the quality of the data is not degraded yet.

3 WATERMARKING METHODS

The basic principle of watermarking methods is to add copyright information into the original data by modifying it in a way that the modifications are perpetual invisible and robust. It is obvious that the watermarking methods may depend on the media type and perhaps also content feature of multimedia documents. The watermarking server presented in this paper employs the methods developed in SysCoP [12]. Currently, three watermarking methods have been developed in SysCoP supporting three important media, namely, still images, motion images and structured text image. All methods share a framework for watermark-embedding or for watermark-retrieval process. Each process is composed of two steps. The first step is to generate a pseudo random position sequence for selecting blocks where the code is embedded, using extracted features of the multimedia data together with a user-supplied secret key as the seeds. The second step simply embeds or retrieves the code into or from the blocks specified in the position sequence using different watermarking methods. Each of these watermarking methods will be outlined below.

Frequency Hopping

The frequency-hopping watermarking method embeds a watermark bit through holding specific relationships between three randomly-selected quantized elements with a moderate variance level in the middle frequency ranges. The relationships among them compose 8 patterns (combinations), which are divided into three groups: "1" patterns and "0" patterns

representing "1"- or "0"-bit of embedded watermark respectively, and the *invalid patterns*. If too big modifications are needed to hold a desired valid pattern representing a bit, this block is invalid. In this case, the relationships among the three elements of the selected location set are modified to any of the invalid patterns, or are stored as part of the secret key to "tell" the watermark-retrieval process that this block is invalid. The criterion for invalid blocks is the maximum difference between any two elements of a selected set in order to reach the desired valid pattern.

By dividing the elements that have moderate variance level in a block into several zones, we can support *hierarchical digital watermarking*, i.e. multiple copyright watermarks can be embedded in different zones, and each of them can be separately extracted later. To increase the robustness of the watermarks, the same watermark can be redundantly embedded into one data more than one times.

Black/White Ratio-based Switching

This method was designed to embed robust watermarks into binary images (i.e. black/white images). A bit is embedded into a randomly selected block in the following way: a "1"-bit is embedded into the block if the ratio of black to white is in a range (T_1), and a "0"-bit is embedded into the block b if the ratio is in another range (T_2). A sequence of randomly selected blocks is modified by switching whites to blacks or vice versa until falling into the ranges. When too much switching is needed, the selected block is invalid and is modified into any invalid range which is outside T_1 and T_2. A "buffer" λ is introduced between T_1, T_2 and the invalid ranges, representing the robustness degree against image processing of watermarked images, i.e. the number of bits that can be altered after image processing without damage of embedded bits.

Line & Word Shifting

This method was developed in AT&T Bell Laboratories [8] and can be used to watermark the text format file (e.g. in Postscript format) or black-white document images. A bit is embedded into a text document by shifting slightly a line down or up, and/or a word in a line left or right. We have implemented a simple version of this method. First we only support a specific format of text document, namely, the Window-Word produced Postscript file, Second we do not use the first and last lines of paragraph, and a line or a word in a line where a bit is embedded is always accompanied by two unmodified lines (one above and one below) or two unmodified words (one left and one right).

4 COPYRIGHT WATERMARK VERIFICATION

The aim of the copyright verification is to claim the ownership and/or identify the original purchaser of a watermarked work. This aim consists of three tasks:

- To construct the embedded codes using the secret key that was used in the watermarking embedding process,
- To prove that a watermark retrieved from a material is the same one that was embedded, and
- To determine which watermarking is earlier than another one.

The first task can be accomplished using a watermarking server or a local watermarking retrieval program. Several approaches have been proposed to prove the authenticity of the watermark, and to determine the watermarking time. They will be described below.

Error Correction

The first approach is to embed an error-correction code, in addition to the information provider's or purchaser's identifier, into the material. The advantage of this approach is that neither additional information nor the involvement of third party is needed in solving copyright disputes. However, trust and reliability of this approach are restricted on the capability of the error-correction method.

Watermark Certificate

The third copyright verification approach is to use a certificate issued by the watermarking server. When a document is registered and marked in a server, the server issues a certificate stamped with its digital signature. In addition, this certificate is encrypted using the requester's public key and therefore can only be decrypted by the requester. The certificate may contain most same information (holder, registration time, embedded watermark, etc.) that are also stored in the server's database. Thus, many copyright disputes may be solved by parties involved according to the rules described above.

Use of a Watermarking Server

In the second approach, a watermarking server takes over the verification task using the original watermarks stored in its database. The automatic verification process at the server consists of three steps, as shown in Figure 2:

(1) Retrieve the embedded code using the user-supplied secret key and the multimedia data to be verified.

(2) Retrieve the watermark from the server's database according to the unique document identification (DID).

(3) Compare two watermarks that are retrieved from the multimedia data and the database, respectively. If the match accuracy is greater than a criteria percentage T (e.g. 85%), the verification succeeds, otherwise fails.

To determine a watermark is earlier than another, both watermarked works are usually needed. We assume that the similarity between two works is judged by human experts – they determine whether a work is derived from the other (i.e. infringes copyrights in the deriving work). Assume that the two similar works in a copyright dispute are d1 and d2 held by the person p1 and p2, respectively. If p1 is able to read his/her valid watermark both from d1 and d2, he/she is supposed to be the "original" owner of the work.

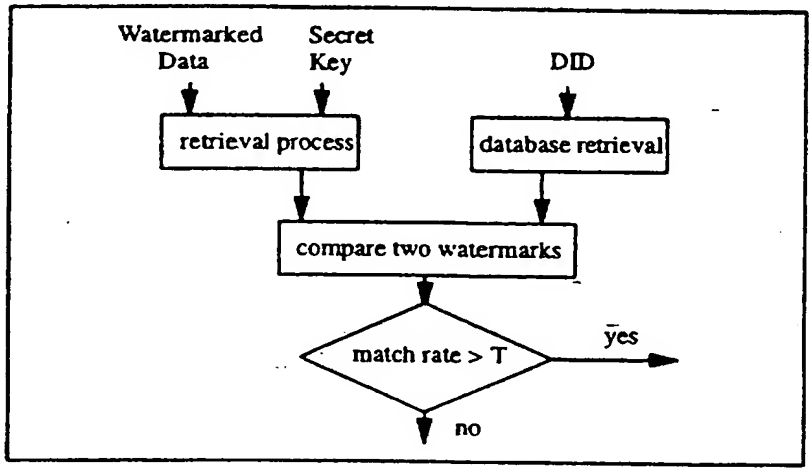

Figure 2. Copyright verification by the Watermarking Server

A watermarking server may also use watermarking time to determine which watermark is "original" if both watermarkings were performed by a server. If both d1 and d2 have been marked and registered by p1 and p2 in watermarking servers, the registration time of d1 and d2 is the decisive factor in solving the dispute: the earlier register shall hold the ownership of d1 and d2.

5 IMPLEMENTATION IN THE WWW

As increasingly expansion and development of the World Wide Web, on the one hand, copyright problem has became one of major barriers in the commercial use of the WWW publishing [13]: without appropriate copyright protection and revenue technologies, the WWW will and can only stay for advertisement purpose in the field of commercial electronic publishing or for disseminating "gray literature" (technical reports and other materials that have not yet been published formally). On the other hand, the WWW provides an excellent means for a wide range of WWW users to perform copyright transactions and for copyright holders and agents to offer electronic services such as clearance, licensing, as well as watermarking and registration. This section describes an implementation of a watermarking

server in the World Wide Web. It accepts the requests from WWW users for copyright watermarking and verification of their copyrighted materials.

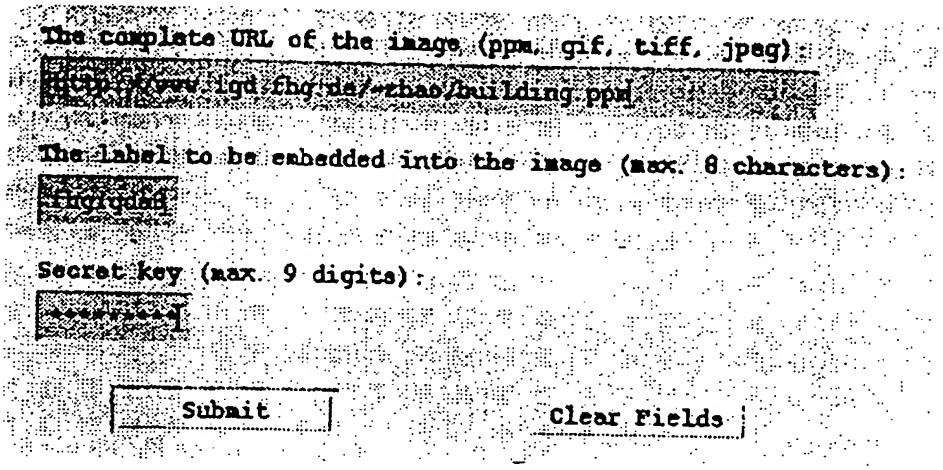

Figure 3. Image watermark-embedding form

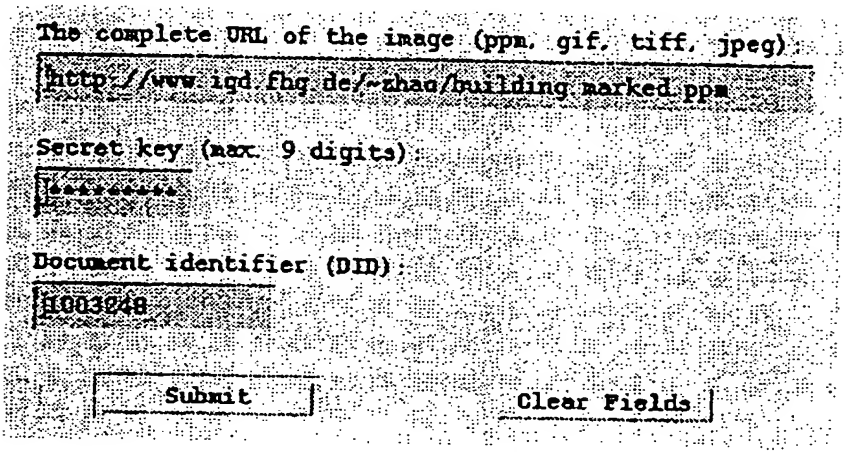

Figure 4. Image watermark-retrieval form

Technically, the WWW user's watermark-embedding or -retrieval requests (in a WWW client) are implemented as two HTML forms, which are shown in Figure 3 and 4, respectively. The complete URL of the multimedia data to be watermarked must be entered in the first field. The server accepts various image formats, including PPM (PGM, PBM), JPEG, GIF, TIFF. Since conversions between image formats do not damage watermarks, any conversion

toolkit (e.g. PBMPLUS or XV) can be used to convert other formats to an acceptable one before sending it to the server. MPEG-1 and the Postscript data produced by Microsoft Window Word are the supported formats for video and structured text, respectively. Up to 8 characters can be entered as a watermark code to designate the copyright information such as owner's ID, purchaser's ID. In the last entry field a secret key must be given.

The "Submit" buttons in the forms activate gateway programs of a secure "httpd" server (Hypertext Transfer Protocol Daemon). The gateway programs communicate with the WWW server/browser using the standard CGI (Common Gateway Interface) [14], and perform the watermark embedding and extraction by calling SysCoP commands and functions. This WWW server together with these gateway programs forms a watermarking server.

The security and trust of the watermarking server mainly rely on a secure "httpd" (e.g. NCSA's s-httpd [15]) and a secure Web browser (e.g. NCSA's secure mosaic [16]). They support authentication, integrity and confidentiality between the service requesters and the watermarking server.

Embedding Watermarks

The watermark-embedding gateway program accomplishes a watermarking request in the following four steps. Figure 5 shows the whole process in respect of data flows between the watermarking server and the requester's WWW client and server.

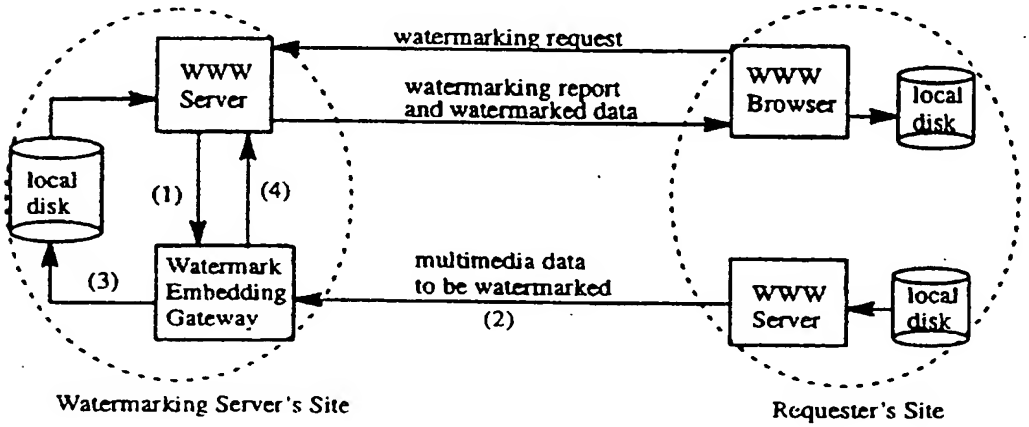

Figure 5. Watermark-embedding process

(1) Get the request-form information using the CGI, including the complete URL (Uniform Resource Locator) of the data to be marked, a secret key, a watermark code to be em-

bedded into the data, and any (optional) additional copyright message (e.g. author, contact address, price, etc.).

(2) Get the multimedia data to be marked according to its complete URL address.

(3) Watermark-embedding transaction. First a unique document identification (DID) is assigned to the multimedia data. Then the gateway program calls the watermark-embedding command which takes the secret key, the watermark and the data as input parameters and produces a marked data file. In addition, this DID is also embedded into the data as the public watermark. Finally, it stores the DID, the embedded watermark, registration information (e.g. registration time, requester name), and the optional copyright message into a secure database.

(4) Create a HTML page which will be shown on the requester's Web browser using CGI protocol. This page reports the status of the watermark-embedding process, shows the DID which has been assigned to uniquely identify the watermarking requester, and displays the marked multimedia data as an accessible icon. The requester click on this icon to get the watermarked data and store it into local disk.

Each watermark-embedding request is stored as a record into a secure database managed by a simple client-server DBMS on the watermarking server. As expansion of the number of watermarking servers, a federated, interoperable database management tool will be needed in the future for data exchange and integration between the databases at different servers. Each record consists of the following information:

- Unique Document Identifier (DID), which uniquely identifies the document in each watermark-embedding request.
- Registration and watermarking time.
- Requester's information, including user name, client address, etc.
- A checksum of the multimedia data.
- Information about watermarked document, including the type, format, and size of the document, and optionally a short description of the document content.
- Watermarking status, which represents the result of the embedding process (e.g. failure reasons).
- Embedded watermark, which is either supplied by the requester or generated by the system if it is not provided.
- Any copyright message which is optionally given the requester.

It is noted that the source and watermarked multimedia data, or the secret key supplied by the user for watermarking each multimedia data is not stored in the watermarking server. In the

current implementation, DID is a number incrementally assigned by the watermarking server – it should be a universal identification number (such as ISBN for books or ISRC for records) harmonized to international standards; The checksum of data could be replaced in the future by a hash value (e.g. produced with a MD5 algorithm) or more efficient feature digest in order to provide document authenticity and integrity service.

Retrieval of Watermarks

The watermark-retrieval gateway program reads a watermark, and verifies the ownership or recipient (if the watermark is secret) or reports the copyright information stored on the watermarking server (if this watermark is public). This process consists of four steps as illustrated in Figure 6:

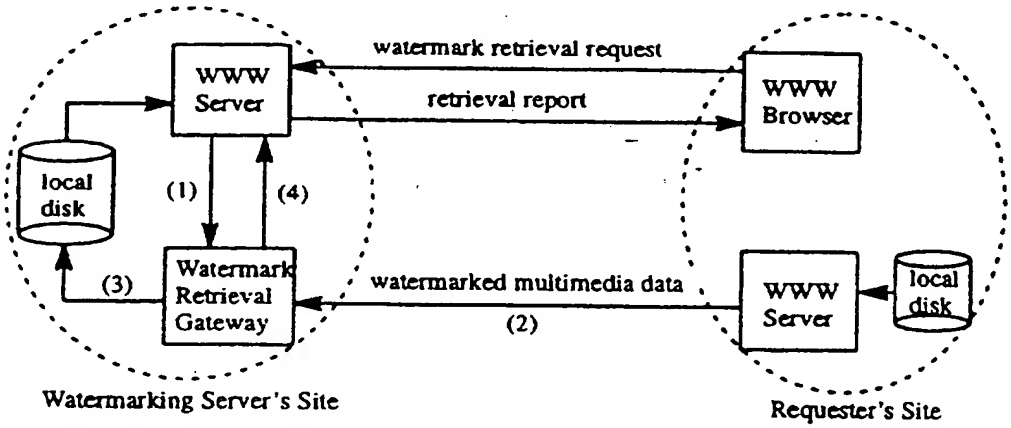

Figure 6. Watermark-retrieval process

(1) Get the request-form information using the CGI, including the complete URL of the watermarked data, a secret key and a DID (only for retrieval of secret watermark).

(2) Get the watermarked data according to its complete URL address.

(3) If a secret key was given, retrieve a watermark using this key and preforms copyright verification as described in Section 4 and illustrated in Figure 2; otherwise use the retrieved public watermark as a DID to search the database on the watermarking server to obtain corresponding copyright messages.

(4) Create a HTML page, and show it on requester's Web browser using CGI protocol. This page displays the retrieved watermark, reports the status of the watermark-retrieval process, and shows the verification result (in case of retrieval of secret watermark), or public copyright message (in case of public watermark retrieval).

6 CONCLUSION

This paper presents a watermarking server providing multimedia copyright-watermarking and -verification services and an implementation in the World Wide Web. This WWW copyright watermarking server has been released to the whole WWW user since October 1995. Hundreds of requests and great attentions from a wide range of perspectives have been received since its operation. The URL of the server is *http://sagittarius.igd.fhg.de:64325*.

The present implementation of the watermarking server on the WWW is only at its very early phase. The further developments will go on in several directions: -

The copyright watermarking scheme discussed in the paper only addresses part of the multimedia chain and actors involved. The static common functional model as well as the dynamic transactional model, which is being developed in the TALISMAN project [17] to cover the whole production and transaction chains of multimedia works, might be taken as a reference model for extensions.

We also plan to integrate and combine the watermarking server with a Copyright Clearance Center, which provides traditional copyright clearing and licensing services, for example, copyright query service (i.e. to determine what rights a user needs and who holds the rights), copyright negotiation and licensing in copyright transactions between the user and "copyright offices".

Though the technology for digital copyright watermarking is still in its early development and there is no legislation at present to accept its legal status, some activities have been under way [4, 18]. We believe that as the digital watermarking technology becomes mature and is widely used, it will obtain an important legal position in a court trial – perhaps just like fingerprint or blood group.

REFERENCES

[1] Samuelson, P. (1991).
Legally Speaking: Digital Media and the Law.
Communications of the ACM, 34(10), October 1991. pp.23-28.

[2] Kahin, B. (1994).
The strategic environment for protecting multimedia. IMA Intellectual Property Project Proceedings, vol. 1, no.1, 1994. pp.1-8.

[3] Koch, E.; Rindfrey, J.; Zhao, J. (1994).
Copyright Protection for Multimedia Data. *Proceedings of the International Conference on Digital Media and Electronic Publishing* (6-8 December 1994, Leeds, UK).

[4] Lehman, B. A. and Brown, R. H. (1995).
Intellectual Property and the National Information Infrastructure.
Section C, Part II, The Report of the Working Group on Intellectual Property Rights, September 1995.

[5] Van Slype, G. (1994).
Natural language version of the generic CITED model. ESPRIT II CITED Project 5469, June 28, 1994.

[6] COPICAT. (1994).
Copyright Ownership Protection in Computer Assisted Training (COPICAT), Esprit Project 8195, Workpackage 2 (Requirements Analysis), Deliverable 1, June 2, 1994.

[7] Samuelson, P. (1995).
Legally Speaking: Copyright and Digital Libraries.
Communications of the ACM, 38(3), April 1995.

[8] Brassil, J.; Low, S.; Maxemchuk, N.; O'Gorman, L. (1994).
Electronic Marking and Identification Techniques to Discourage Document Copying. AT&T Bell Laboratories, Murray Hill, NJ, 1994.

[9] Van Schyndel, R.G.; Tirkel, A.Z.; Osborne, C.F. (1994). A digital watermark.
In: Int. Conf. on Image Processing, vol. 2, page 86-90, 1994.

[10] Macq, B and Quisquater, J. J. (1995).
Cryptology for Digital TV Broadcasting.
In: Proc. of the IEEE, vol. 83, no. 6, 1995, pp. 944-957.

[11] Cox, I.J.; Kilian, J.; Leighton, T.; Shamoon, T.
Secure Spread Spectrum Watermarking for Multimedia.
Princeton, NJ: NEC Research Institute, Technical Report 95-10, October 1995.

[12] Zhao, J. and Koch, E. (1995).
Embedding Robust Labels Into Images For Copyright Protection.
In: Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies (Vienna, Austria, August 21-25, 1995).

[13] Norderhaug, T. and Oberding, J. M. (1995).
Designing a Web of Intellectual Property.
In: Proc. of the Third International World-Wide Web Conference (10-14 April 1995, Darmstadt, Germany). pp.1037-1046.

[14] CGI.
The Common Gateway Interface. See http://hoohoo.ncsa.uiuc.edu/cgi/overview.html.

[15] Shttpd.
The Secure NCSA httpd. See http://www.commerce.net/software/Shttpd.

[16] SMosaic.
The Secure NCSA Mosaic. See http://www.commerce.net/software/SMosaic.

[17] TALISMAN. (1996).
Common Funtional Model. Workpackage 1 of the TALISMAN project (EC ACTS AC019), Deliverable 12, February 1996.

[18] EC-COM(95)-382.
The Green Paper of Copyright and Related Rights in the Information Society.
Section 9, Part 2, Commission of the European Communities, COM(95) 382 final, Brussels, 19 July 1995.